

10/531713

PCT/PTO 18 APR 2005

特 許 協 力 条 約

PCT

特許性に関する国際予備報告 (特許協力条約第二章)

(法第12条、法施行規則第56条)  
[PCT36条及びPCT規則70]

REC'D 10 JUN 2004

WIPO PCT

出願人又は代理人 の書類記号 P32091-P0	今後の手続きについては、様式PCT/IPEA/416を参照すること。	
国際出願番号 PCT/JP03/13218	国際出願日 (日.月.年) 15. 10. 2003	優先日 (日.月.年) 17. 10. 2002
国際特許分類 (IPC) Int. Cl <sup>7</sup> H04L12/56		
出願人 (氏名又は名称) 松下電器産業株式会社		

1. この報告書は、PCT35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。  
法施行規則第57条 (PCT36条) の規定に従い送付する。

2. この国際予備審査報告は、この表紙を含めて全部で 6 ページからなる。

3. この報告には次の附属物件も添付されている。

a ☒ 附属書類は全部で 18 ページである。

☒ 補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び/又は図面の用紙 (PCT規則70.16及び実施細則第607号参照)

☐ 第I欄4. 及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b ☐ 電子媒体は全部で \_\_\_\_\_ (電子媒体の種類、数を示す)。  
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。(実施細則第802号参照)

4. この国際予備審査報告は、次の内容を含む。

☒ 第I欄 国際予備審査報告の基礎

☐ 第II欄 優先権

☐ 第III欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成

☐ 第IV欄 発明の単一性の欠如

☒ 第V欄 PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明

☐ 第VI欄 ある種の引用文献

☐ 第VII欄 国際出願の不備

☐ 第VIII欄 国際出願に対する意見

国際予備審査の請求書を受理した日 05. 02. 2004	国際予備審査報告を作成した日 20. 05. 2004	
名称及びあて先 日本国特許庁 (IPEA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員)  五木 宏治	5X 3047
電話番号 03-3581-1101 内線 3596		

様式PCT/IPEA/409 (表紙) (2004年1月)

## 第I欄 報告の基礎

1. この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

- ☐ この報告は、\_\_\_\_\_語による翻訳文を基礎とした。  
それは、次の目的で提出された翻訳文の言語である。
- ☐ PCT規則12.3及び23.1(b)にいう国際調査
- ☐ PCT規則12.4にいう国際公開
- ☐ PCT規則55.2又は55.3にいう国際予備審査

2. この報告は下記の出願書類を基礎とした。(法第6条(PCT14条)の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。)

☐ 出願時の国際出願書類

☒ 明細書

第 1-76 \_\_\_\_\_ ページ、  
第 \_\_\_\_\_ ページ\*、  
第 \_\_\_\_\_ ページ\*、

出願時に提出されたもの

付で国際予備審査機関が受理したもの  
付で国際予備審査機関が受理したもの

☒ 請求の範囲

第 \_\_\_\_\_ 項、  
第 \_\_\_\_\_ 項\*、  
第 52-98 \_\_\_\_\_ 項\*、  
第 \_\_\_\_\_ 項\*、

出願時に提出されたもの

PCT19条の規定に基づき補正されたもの

14.05.2004

付で国際予備審査機関が受理したもの  
付で国際予備審査機関が受理したもの

☒ 図面

第 1-38 \_\_\_\_\_ ページ/図、  
第 \_\_\_\_\_ ページ/図\*、  
第 \_\_\_\_\_ ページ/図\*、

出願時に提出されたもの

付で国際予備審査機関が受理したもの  
付で国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル

配列表に関する補充欄を参照すること。

3. ☒ 補正により、下記の書類が削除された。

- ☐ 明細書 第 \_\_\_\_\_ ページ
- ☒ 請求の範囲 第 1-51 \_\_\_\_\_ 項
- ☐ 図面 第 \_\_\_\_\_ ページ/図
- ☐ 配列表 (具体的に記載すること)
- ☐ 配列表に関連するテーブル (具体的に記載すること) \_\_\_\_\_

4. ☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c))

- ☐ 明細書 第 \_\_\_\_\_ ページ
- ☐ 請求の範囲 第 \_\_\_\_\_ 項
- ☐ 図面 第 \_\_\_\_\_ ページ/図
- ☐ 配列表 (具体的に記載すること)
- ☐ 配列表に関連するテーブル (具体的に記載すること) \_\_\_\_\_

\* 4. に該当する場合、その用紙に "superseded" と記入されることがある。

第V欄 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

## 1. 見解

新規性(N)

請求の範囲 52-98

請求の範囲

有  
無

進歩性(IS)

請求の範囲 68, 70, 71, 74, 94-98

請求の範囲 52-67, 69, 72, 73, 75-93

有  
無

産業上の利用可能性(IA)

請求の範囲 52-98

請求の範囲

有  
無

## 2. 文献及び説明(PCT規則70.7)

文献1: JP 2002-202720 A (株式会社東芝)  
2002.07.19 要約

文献2: JP 2000-341324 A (株式会社エヌ・ティ・ティ・データ)  
2000.12.08 第0002段落, 第0003段落

文献3: JP 7-79252 A (富士通株式会社)  
1995.03.20 要約

文献4: JP 8-130543 A (日本電信電話株式会社)  
1996.05.21 要約

文献5: JP 2000-299686 A (日本電気株式会社)  
2000.10.24 要約

文献6: JP 2002-26906 A (三菱電機株式会社)  
2002.01.25 第0036段落, 第0037段落

文献7: JP 7-297831 A (住友電気工業株式会社)  
1995.11.10 第0038段落

文献8: 高田 学也, 三輪 芳久, “特集2 インターネットの基盤  
「IPを知る」”, 日経ネットワーク, 日経BP社, 第30号,  
2002.09.22, pp.124-139  
“役割3 パケットを分割する 通る回線に合わせて大きさを調整”  
(pp.132-135)

文献9: JP 11-196081 A (株式会社高度移動通信  
セキュリティ技術研究所) 1999.07.21 第0003段落

## 補充欄

いずれかの欄の大きさが足りない場合

## 第 V.2 欄の続き

文献10: 山本 喜一, 西野 謙一, 高橋 哲也, 「通信コスト削減の武器としてのVPN」, INTEROP MAGAZINE, ソフトバンクパブリッシング株式会社, 第9巻, 第8号, 1999. 10. 01, pp. 44-51  
p. 48左欄第32行目から第35行目

文献11: JP 2002-217961 A (富士通株式会社)  
2002. 08. 02 請求項2

文献12: JP 2001-186173 A (松下電器産業株式会社)  
2001. 07. 06 第0153段落

文献13: JP 2002-232955 A (株式会社デンソー)  
2002. 08. 16 請求項1-3

文献14: JP 2001-86110 A (東洋通信機株式会社)  
2001. 03. 30 第0005段落, 第9図

・請求の範囲 52-54, 65-67, 75-77, 80-82

上記文献1, 2のそれぞれには, 送信装置と受信装置との間で, 鍵交換を行い, 当該鍵交換によって交換された鍵に基づいて, データを暗号化して送受信することが記載されている。

そして, 送信アドレスなどの送信関連情報, MACアドレスなどの送受信管理情報などを用いて, パケットを生成することは, IP網において, 一般的に行われていることである。

また, 文献3, 4には, バッファの蓄積量がしきい値を超えると, 当該バッファからのデータを優先的に出力することが記載されている。

蓄積量がしきい値を超えたとき, データを優先的に出力して, 蓄積量がしきい値を下回るように制御することは, 蓄積量がしきい値を超えないように制御することに他ならない。

上記文献5には, パケットを複数のクラスのキューに蓄積し, 前記クラスに割り当てられた帯域情報に基づいて, 各キューに蓄積されたパケットを出力することが記載されている。

・請求の範囲 55-64

上記文献6には, 重要度の高いデータは暗号化し, 重要度の低いデータは暗号化しないで送信することが記載されている。

データの転送レートが所定の値より小さくならないように制御することは, シェーピング等で一般的に行われていることである。

## 補充欄

いずれかの欄の大きさが足りない場合

## 第 V.2 欄の続き

## ・請求の範囲 60

上記文献7には、残り蓄積可能時間を超えないように、すなわち、蓄積される時間があらかじめ決めた値より小さくなるように、データを出力することが記載されている。

## ・請求の範囲 61-64, 79

上記文献8には、送信装置から受信装置までの伝送路において伝送可能な最大パケット長を調査して、当該最大パケット長でデータを伝送することが記載されている。

そして、伝送するパケットのパケット長や、エラー訂正用のデータをパケットに付加することは、一般的に行われていることである。

## ・請求の範囲 69, 73, 90, 93

上記文献9には、鍵を一定時間使用すると、鍵の更新を行うことが記載されている。

どのようなプロトコルにおいて、一定時間毎に鍵を更新するかは、当該技術分野の専門家であれば、適宜決定できた設計的事項であり、プロトコルとして周知のRTPを採用することに格別の困難性は認められない。

## ・請求の範囲 72, 92

上記文献10には、一定のデータ量毎に鍵を更新することが記載されている。

どのようなプロトコルにおいて、一定のデータ量毎に鍵を更新するかは、当該技術分野の専門家であれば、適宜決定できた設計的事項であり、プロトコルとして周知のHTTPを採用することに格別の困難性は認められない。

## ・請求の範囲 78

上記文献11には、複数のキューから均等に、パケットを出力することが記載されている。

## ・請求の範囲 83, 84

上記文献12には、パケットの優先度のためのフィールドとして、IPv4パケットのTOSフィールド、IPv6パケットのトラフィッククラスのフィールドを用いることが記載されている。

## ・請求の範囲 85-89

上記文献13には、移動端末の位置情報に基づいて認証を行い、認証の結果が否であればパスワードによる認証を行うことが記載されている。

そして、パスワードによる認証に代えて、証明書等で認証を行うように構成することは、当該技術分野の専門家であれば容易に成し得たことである。

## 補充欄

いずれかの欄の大きさが足りない場合

## 第 V.2 欄の続き

## ・請求の範囲 91

上記文献14には、送信パケットに鍵の変更タイミングを付加することが記載されている。

## ・請求の範囲 68

上記文献1-14のいずれにも、暗号鍵を示す情報を、送信フレームの送信から当該送信フレームに対応する受信フレームの受信までの時間より前に送信することは記載も示唆もされていない。

## ・請求の範囲 70, 71, 74, 96, 97

上記文献1-14のいずれにも、鍵更新のタイミングをシーケンス番号に同期したタイミングとすること、HTTPリクエスト毎に更新すること、エラー訂正マトリックスの終点または始点に同期したタイミングとすること、該タイミングを、ポート番号の変化によって通知することは記載も示唆もされていない。

## ・請求の範囲 94, 95

上記文献1-14のいずれにも、パケットの片道もしくは往復の伝播遅延時間や、スクランブルして伝送するモードであるか否かに基づいて認証を行うことは記載も示唆もされていない。

## ・請求の範囲 98

上記文献1-14のいずれにも、DTCP方式のコピー制御情報は、送信パケットに暗号化モード情報を付加することで伝送することは、記載も示唆もされていない。

請求の範囲

1. (削除)
2. (削除)
3. (削除)
- 5 4. (削除)
5. (削除)
6. (削除)
7. (削除)
8. (削除)
- 10 9. (削除)
10. (削除)
11. (削除)
12. (削除)
13. (削除)
- 15 14. (削除)
15. (削除)
16. (削除)
17. (削除)
18. (削除)
- 20 19. (削除)
20. (削除)
21. (削除)
22. (削除)
23. (削除)
- 25 24. (削除)
25. (削除)

- 2 6. (削除)
- 2 7. (削除)
- 2 8. (削除)
- 2 9. (削除)
- 5 3 0. (削除)
- 3 1. (削除)
- 3 2. (削除)
- 3 3. (削除)
- 3 4. (削除)
- 10 3 5. (削除)
- 3 6. (削除)
- 3 7. (削除)
- 3 8. (削除)
- 3 9. (削除)
- 15 4 0. (削除)
- 4 1. (削除)
- 4 2. (削除)
- 4 3. (削除)
- 4 4. (削除)
- 20 4 5. (削除)
- 4 6. (削除)
- 4 7. (削除)
- 4 8. (削除)
- 4 9. (削除)
- 25 5 0. (削除)
- 5 1. (削除)



5 2. (追加) 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

5 前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

10 前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

15 前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段と、

20 前記パケット化手段にて生成された第1のパケットを一時的に蓄積する第1のキュー手段と、

前記パケット化手段にて生成された第2のパケットを一時的に蓄積する第2のキュー手段と、

25 前記送信条件設定情報に基づいて、前記第1のキュー手段に蓄積された前記第1のパケットおよび前記第2のキュー手段に蓄積された前記第2のパケットのいずれを送信するかを制御する送信キュー制御手段と、

前記第 1 のキュー手段から出力された第 1 のパケットおよび第 2 のキュー手段から出力された第 2 のパケットをフレーム化することによって送信フレームを生成するフレーム化手段と、

受信フレームから前記受信パケットを抽出するフレーム受信手段と  
5 を備え、

前記送信キュー制御手段は、前記第 2 のキュー手段に蓄積された前記第 2 のパケットの量が所定の量を超えないように前記第 2 のキュー手段に蓄積された前記第 2 のパケットが出力されるように、前記第 1 のキュー手段および前記第 2 のキュー手段を制御する、パケット送受信装置。

10 5 3. (追加) 前記パケット化手段は、第 1 のパケット化手段と、第 2 のパケット化手段とを含み、

前記第 1 のパケット化手段は、前記送信条件設定情報および前記認証・鍵交換関連情報の少なくとも一つの情報を用いて前記第 1 のパケットを生成し、

15 前記第 2 のパケット化手段は、前記送信条件設定情報と、前記認証・鍵交換関連情報と、前記暗号化送信データとの少なくとも一つの情報を用いて前記第 2 のパケットを生成する、請求の範囲第 5 2 項に記載のパケット送受信装置。

20 5 4. (追加) 前記パケット化手段は、前記暗号化送信データを所定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIPヘッダを付加し、

前記第 1 のパケット化手段はソフトウェアによって構成され、前記第 2 のパケット化手段はハードウェアによって構成される、請求の範囲第 5 3 項に記載のパケット送受信装置。

25 5 5. (追加) 前記送信データを優先データと一般データとに分離するデータ

分離手段をさらに備え、

前記暗号化手段は、前記優先データを暗号化し、

前記第1の packets 化手段は、前記一般データを用いて第1の packets を生成する、請求の範囲第53項に記載の packets 送受信装置。

5

56. (追加) 前記第1の packets 化手段は、IETF文書で規定されているデータ処理プロトコルであるRTCP, RTSP, HTTP, TCP, UDP, IPのうちの少なくとも1つのヘッダを付加する、請求の範囲第55項に記載の packets 送受信装置。

10

57. (追加) 前記第2の packets 化手段は、データにシーケンス番号を付加するか、または、IETF文書で規定されているデータ処理プロトコルであるRTP, UDP, HTTP, TCP, IPのうちの少なくとも1つのヘッダを付加する、請求の範囲第55項に記載の packets 送受信装置。

15

58. (追加) 前記優先データは、SMPTE 259M規格で規定された非圧縮SD方式信号、または、SMPTE 292M規格で規定された非圧縮HD形式、または、IEC 61883規格で規定されたIEEE1394によるDVまたはMPEG-TSの伝送ストリーム形式、または、DVB-ASIによるMPEG-TS形式、MPEG-PS形式、MPEG-ES形式、MPEG-PE  
20 ES形式の内の少なくとも一つのデータストリーム形式またはデータファイル形式である、請求の範囲第55項に記載の packets 送受信装置。

20

59. (追加) 前記優先データのデータレートが所定の値より小さくならない  
25 ように、前記送信キュー制御手段は前記第1のキュー手段および前記第2のキュー手段を制御する、請求の範囲第55項に記載の packets 送受信装置。

25

60. (追加) 前記送信キュー制御手段は、前記優先データが前記第2のキュー手段に蓄積される時間があらかじめ決めた値より常に小さくなるように、前記送信キュー制御手段は前記第1のキュー手段および前記第2のキュー手段を制御する、請求の範囲第59項に記載のネットワーク送受信装置。

61. (追加) 前記第2のネットワーク化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、前記第2のネットワークのネットワークヘッダを生成するネットワークヘッダ生成手段と、前記ネットワークヘッダと前記バッファから出力されるペイロードとを組み合わせるネットワーク合成手段とを含み、

前記ネットワークヘッダ生成手段は前記第2のネットワークのペイロード長を指定して、前記バッファ手段に蓄積されたデータを読み出して、前記ネットワーク合成手段に入力する、請求の範囲第59項に記載のネットワーク送受信装置。

62. (追加) 前記第2のネットワーク化手段は、前記優先データから抽出したデータを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、ネットワーク化情報を用いてネットワークヘッダを生成するネットワークヘッダ生成手段と、前記ネットワークヘッダとペイロードとを組み合わせるネットワーク生成手段とを含み、

前記カウンタ手段は前記バッファ手段からペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第59項に記載のネットワーク送受信装置。

63. (追加) 前記第2のネットワーク化手段は、データを一時的に蓄積するバッファ手段と、前記データの長さをカウントするカウンタ手段と、ネットワーク化情報

を用いてパケットヘッダを生成するパケットヘッダ生成手段と、前記データにエラー訂正を付加するエラー訂正付加手段と、前記パケットヘッダと前記エラー訂正を付加したデータとを合成するパケット合成手段とを含み、

5 前記カウンタ手段は前記バッファ手段よりペイロード長に相当するデータを読み出すための制御データを出力する、請求の範囲第59項に記載のパケット送受信装置。

10 64. (追加) 前記優先データおよび前記一般データが処理されるレイヤよりも下位レイヤの受信フレームを処理するレイヤにおいて、前記受信フレームに含まれる受信パケットの通信プロトコルヘッダから前記優先データと前記一般データを選別して、前記優先データの処理と前記一般データの処理を独立に行う、請求の範囲第59項に記載のパケット送受信装置。

15 65. (追加) 前記第2のパケット化手段は、エラー訂正符号付加手段を含む、請求の範囲第53項に記載のパケット送受信装置。

20 66. (追加) 前記エラー訂正符号付加手段で用いられるエラー訂正符号の方式は、リードソロモン方式、あるいはパリティ方式である、請求の範囲第65項に記載のパケット送受信装置。

25 67. (追加) 前記暗号化鍵を示す情報は、前記フレーム化手段において前記暗号化鍵で暗号化された送信パケットを出力するより前に、前記暗号化鍵の復号情報を前記フレーム化手段から出力する、請求の範囲第53項に記載のパケット送受信装置。

68. (追加) 前記暗号化鍵を示す情報は、前記暗号化鍵を用いて生成された

前記暗号化送信データを含む送信パケットが送信されるときよりも、前記送信フレームの送信から前記送信フレームに対応する受信フレームの受信までの時間より前に送信される、請求の範囲第67項に記載のパケット送受信装置。

5      69. (追加) 前記第2のパケット化手段は、暗号鍵切替手段を含み、前記暗号鍵切替手段に入力される暗号鍵を指定されたタイミングで切り替えながら前記暗号化手段に入力し、前記暗号化手段における暗号化鍵を指定の間隔で切替る、請求の範囲第53項に記載のパケット送受信装置。

10     70. (追加) 前記暗号鍵切替に用いるタイミングとしては、前記パケットヘッダ生成手段の出力であるパケットヘッダ内の所定のシーケンス番号に同期して発生したタイミングである、請求の範囲第69項に記載のパケット送受信装置。

15     71. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがHTTPを使用している場合、HTTPリクエスト毎に更新される、請求の範囲第69項に記載のパケット送受信装置。

20     72. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがHTTPを使用している場合、一定のデータ量毎に変化される、請求の範囲第69項に記載のパケット送受信装置。

25     73. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがRTPを使用している場合、予め決められた期間内に更新される、請求の範囲第69項に記載のパケット送受信装置。

74. (追加) 前記暗号鍵切替に用いるタイミングとしては、エラー訂正マト

リックスの終点または始点に同期して発生したタイミングである、請求の範囲第 69 項に記載の packets 送受信装置。

75. (追加) 前記送信キュー制御手段は、前記第 1 の packets または前記第 2 の packets の送信経路に関する情報と、前記第 1 の packets または前記第 2 の packets を送信するのに必要な帯域幅に関する情報と、前記送信 packets の送信から到着までの遅延に関する情報と、前記第 1 の packets または前記第 2 の packets の優先度に関する情報とのうち少なくとも 1 つの情報をを用いて、前記第 1 のキュー手段に蓄積された前記第 1 の packets および前記第 2 のキュー手段に蓄積された前記第 2 の packets のいずれを送信するかを制御する、請求の範囲第 52 項に記載の packets 送受信装置。

76. (追加) 前記送信キュー制御手段は、IETF rfc 2205、rfc 2208、rfc 2209 で記載された RSVP 方式、IETF rfc 2210、rfc 2211、2212、rfc 2215 で記載された Intserv 方式、IETF rfc 2474、rfc 2475、rfc 2597、rfc 2598 で記載された DiffServ 方式のいずれか 1 つの制御方式を使用する、請求の範囲第 75 項に記載の packets 送受信装置。

77. (追加) 前記送信キュー制御手段は、前記第 1 のキュー手段に蓄積された前記第 1 の packets および前記第 2 のキュー手段に蓄積された前記第 2 の packets のうちのいずれかを選択して、選択した packets を優先的に出力するように前記第 1 のキュー手段および前記第 2 のキュー手段を制御する、請求の範囲第 52 項に記載の packets 送受信装置。

78. (追加) 前記送信キュー制御手段は、前記第 1 のキュー手段から送信さ

れる前記第1の packets と前記第2のキュー手段から送信される前記第2の packets との間隔を平均化するように前記第1のキュー手段および前記第2のキュー手段を制御する、請求の範囲第52項に記載の packets 送受信装置。

- 5        79. (追加) 前記送信条件設定管理手段および前記受信条件設定管理手段は、前記送信フレームの送信から到着するまでの間において前記送信 packets の送信先から受信先までの経路における最大伝送 packets サイズの検出を行ない、前記最大伝送 packets サイズ情報を用いて、前記送信条件設定情報および前記受信条件設定情報を生成する、請求の範囲第52項に記載の packets 送受信装置。

10

80. (追加) 前記フレーム化手段は、前記 packets 化手段にて生成された前記送信 packets に、IEEE 802.3規格のフレームヘッダを付加する、請求の範囲第52項に記載の packets 送受信装置。

15

81. (追加) 前記フレーム化手段は、前記 packets 化手段にて生成された前記送信 packets に、IEEE 802.1Q規格のフレームヘッダを付加する、請求の範囲第52項に記載の packets 送受信装置。

20

82. (追加) 前記 packets 化手段は、前記暗号化送信データを所定の大きさに変換し、IETFでIPv4またはIPv6として規定されているIP (Internet Protocol) ヘッダを付加する、請求の範囲第52項に記載の packets 送受信装置。

25

83. (追加) 前記 packets 化手段は、IPv4ヘッダのサービスタイプフィールド、または、サービスタイプフィールド内のTOS (Type of Service) フィールドに優先 packets であることを示す情報を付加する、請求



の範囲第52項に記載のケット送受信装置。

84. (追加) 前記ケット化手段は、IPv6ヘッダのプライオリティフィールドに優先ケットであることを示す情報を付加する、請求の範囲第52項に記載のケット送受信装置。

85. (追加) 前記認証・鍵交換手段は、前記ケット送受信装置の位置情報と、前記送信ケットの到着先の位置情報または前記受信ケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可する、請求の範囲第52項に記載のケット送受信装置。

86. (追加) 前記送受信管理情報は、前記ケット送受信装置の位置情報と、前記送信ケットの到着先の位置情報または前記受信ケットの送信元の位置情報との少なくとも一方を含んでいる、請求の範囲第85項に記載のケット送受信装置。

87. (追加) 前記位置情報は、地域コード、住所、郵便番号、または、経度・緯度により範囲が指定された情報である、請求の範囲第86項に記載のケット送受信装置。

88. (追加) 前記認証・鍵交換手段は、

前記ケット送受信装置と、前記送信ケットの到着先または前記受信ケットの送信元との間で認証を行った場合に、前記送信ケットの到着先または前記受信ケットの送信元に関する情報を一時的に記憶する記憶手段と、

前記ケット送受信装置と、前記送信ケットの到着先または前記受信ケットの送信元とが前記あらかじめ決められた条件に合致しないために前記認証が成

立しない場合に、前記記憶手段にて記憶された情報と、前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報とを照合し、前記パケット送受信装置と前記送信パケットの到着先または前記受信パケットの送信元との間で認証を行う、照合手段と

5 を含む、請求の範囲第85項に記載のパケット送受信装置。

89. (追加) 前記送信パケットの前記到着先に関する情報または前記受信パケットの前記送信先に関する情報は、証明書、MACアドレスおよび生体情報の少なくとも1つを含む、請求の範囲第88項に記載のパケット送受信装置。

10

90. (追加) 前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期間で暗号化鍵または復号鍵を更新する、請求の範囲第52項に記載のパケット送受信装置。

15

91. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングを示すタイミング情報が、前記送信パケットに付加される、請求の範囲第90項に記載のパケット送受信装置。

20

92. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがHTTPを使用している場合、一定のデータ量毎に変化される、請求の範囲第90項に記載のパケット送受信装置。

25

93. (追加) 前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットがRTPを使用している場合、予め決められた期間内に更新される、請求の範囲第90項に記載のパケット送受信装置。

94. (追加) 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段とを備え、

前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可し、

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間で、前記パケット送受信装置から前記送信パケットの到着先または前記受信パケットの受信元までの片道または往復

の伝播時間があらかじめ決められた制限時間より短い時間である場合に、認証を許可する、パケット送受信装置。

95. (追加) 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

前記復号鍵を用いて前記受信データを復号する復号手段とを備え、

前記認証・鍵交換手段は、前記パケット送受信装置の位置情報と、前記送信パケットの到着先の位置情報または前記受信パケットの送信元の位置情報とが、あらかじめ決められた条件に合致する時に、認証を許可し、

前記認証・鍵交換手段は、前記パケット送受信装置と、前記送信パケットの到着先または前記受信パケットの送信元との間の送受信区間において無線伝送区間が存在する場合、前記無線伝送区間ではデータをスクランブルして伝送するモードであることを確認した場合に、認証を許可する、パケット送受信装置。

5

96. (追加) 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

10

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

15

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

20

前記復号鍵を用いて前記受信データを復号する復号手段と  
を備え、

25

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パケットのTCPポート番号、またはUDPポート番号を変化させることによって通知される、パケット送受信装置。

5

97. (追加) 送信パケットを送信し、受信パケットを受信するパケット送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

10

前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パケットの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

15

前記暗号化送信データを用いて、前記送信パケットを生成するパケット化手段と、

受信条件関連情報およびパケット受信情報の少なくとも一方を用いて、前記受信パケットの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

20

前記受信パケットを受信するパケット受信手段であって、前記受信条件設定情報を用いて、前記受信パケットから、前記受信パケットに含まれる受信データを抽出するとともに、前記受信パケットから前記パケット受信情報を生成し、前記パケット受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パケット受信手段と、

25

前記復号鍵を用いて前記受信データを復号する復号手段とを備え、

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段が前記復号鍵を更新するタイミングは、前記送信パッケージがHTTPを使用している場合、HTTPリクエスト毎に更新される、パッケージ送受信装置。

5

98. (追加) 送信パッケージを送信し、受信パッケージを受信するパッケージ送受信装置であって、

暗号化鍵および復号鍵を生成する認証・鍵交換手段と、

10 前記暗号化鍵を用いて送信データを暗号化することによって暗号化送信データを生成する暗号化手段と、

前記送信条件関連情報と、送受信管理情報と、受信条件設定情報との少なくとも1つを用いて、前記送信パッケージの送信条件を設定するための送信条件設定情報を生成する送信条件設定管理手段と、

15 前記暗号化送信データを用いて、前記送信パッケージを生成するパッケージ化手段と、

受信条件関連情報およびパッケージ受信情報の少なくとも一方を用いて、前記受信パッケージの受信条件を設定する受信条件設定情報を生成する受信条件設定管理手段と、

20 前記受信パッケージを受信するパッケージ受信手段であって、前記受信条件設定情報を用いて、前記受信パッケージから、前記受信パッケージに含まれる受信データを抽出するとともに、前記受信パッケージから前記パッケージ受信情報を生成し、前記パッケージ受信情報を前記認証・鍵交換手段または前記受信条件設定管理手段に出力する、パッケージ受信手段と、

25 前記復号鍵を用いて前記受信データを復号する復号手段とを備え、

前記認証・鍵交換手段は、予め規定された認証および鍵交換を行い、所定の期

間で暗号化鍵または復号鍵を更新し、

前記認証・鍵交換手段がD T C P方式の場合、コピー制御情報は、前記送信パケットに暗号化モード情報を付加することによって伝送される、パケット送受信装置。



Translation

PATENT COOPERATION TREATY

PCT/JP2003/013218



PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY  
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P32091-P0	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. PCT/JP2003/013218	International filing date (day/month/year) 15 October 2003 (15.10.2003)	Priority date (day/month/year) 17 October 2002 (17.10.2002)
International Patent Classification (IPC) or national classification and IPC H04L 12/56, 9/00		
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
  - a. ☒ (sent to the applicant and to the International Bureau) a total of 18 sheets, as follows:
    - ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
    - ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
  - b. ☐ (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) \_\_\_\_\_, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:

<input checked="" type="checkbox"/> Box No. I	Basis of the report
<input type="checkbox"/> Box No. II	Priority
<input type="checkbox"/> Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
<input checked="" type="checkbox"/> Box No. IV	Lack of unity of invention
<input type="checkbox"/> Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
<input type="checkbox"/> Box No. VI	Certain documents cited
<input type="checkbox"/> Box No. VII	Certain defects in the international application
<input type="checkbox"/> Box No. VIII	Certain observations on the international application

Date of submission of the demand 05 February 2004 (05.02.2004)	Date of completion of this report 20 May 2004 (20.05.2004)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.

PCT/JP2003/013218

## Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

- ☐ This report is based on translations from the original language into the following language \_\_\_\_\_, which is language of a translation furnished for the purpose of:
- ☐ international search (under Rules 12.3 and 23.1(b))
  - ☐ publication of the international application (under Rule 12.4)
  - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

- ☐ The international application as originally filed/furnished
- ☒ the description:
- pages \_\_\_\_\_ 1-76 \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☒ the claims:
- pages \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_, as amended (together with any statement) under Article 19
- pages\* 52-98 received by this Authority on 14 May 2004 (14.05.2004)
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☒ the drawings:
- pages \_\_\_\_\_ 1-38 \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☒ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☒ the claims, Nos. \_\_\_\_\_ 1-51 \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (*specify*): \_\_\_\_\_
- ☐ any table(s) related to sequence listing (*specify*): \_\_\_\_\_

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (*specify*): \_\_\_\_\_
- ☐ any table(s) related to sequence listing (*specify*): \_\_\_\_\_

\* If item 4 applies, some or all of those sheets may be marked "superseded."

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

## 1. Statement

Novelty (N)	Claims	52-98	YES
	Claims		NO
Inventive step (IS)	Claims	68, 70, 71, 74, 94-98	YES
	Claims	52-67, 69, 72, 73, 75-93	NO
Industrial applicability (IA)	Claims	52-98	YES
	Claims		NO

## 2. Citations and explanations (Rule 70.7)

- Document 1: JP, 2002-202720, A (Toshiba Corporation), July 19, 2002 (07.19.02), Abstract
- Document 2: JP, 2000-341324, A (NTT Data Corporation), December 8, 2000 (12.08.00), Paragraph Nos. [0002] and [0003]
- Document 3: JP, 7-79252, A (Fujitsu Limited), March 20, 1995 (03.20.95), Abstract
- Document 4: JP, 8-130543, A (Nippon Telegraph and Telephone Corporation), May 21, 1996 (05.21.96), Abstract
- Document 5: JP, 2000-299686, A (NEC Corporation), October 24, 2000 (10.24.00), Abstract
- Document 6: JP, 2002-26906, A (Mitsubishi Electric Corporation), January 25, 2002 (01.25.02), Paragraph Nos. [0036] and [0037]
- Document 7: JP, 7-297831, A (Sumitomo Electric Industries, Ltd.), November 10, 1995 (11.10.95), Paragraph No. [0038]
- Document 8: Manabu TAKADA, Yoshihisa MIWA, "Tokushu 2, Internet no Kiban "IP wo Shiru," Nikkei Network, Nikkei BP, Vol. 30, September 22, 2002 (09.22.02), pp.124-139, "Yakuwari 3, Packet wo Bunkatsu suru Toru Kaisen ni Awasete Okisa wo Chosei," (pp.132-135)
- Document 9: JP, 11-196081, A (K.K. Kodo Idotsushin Security Gijutsu Kenkyusho), July 21, 1999 (07.21.99), Paragraph No. [0003]

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.  
Continuation of Box V.2:

Document 10: Yoshikazu YAMAMOTO, Kenichi NISHINO, Tetsuya TAKAHASHI, "Tsushin Cost Sakugen no Buki to shite no VPN," Interop Magazine, Soft Bank Publishing Kabushiki Kaisha, Vol.9, No.8, October 1, 1999 (10.01.99), pp.44-51, p.48, left column, lines 32 to 35

Document 11: JP, 2002-217961, A (Fujitsu Limited), August 2, 2002 (08.02.02), Claim 2

Document 12: JP, 2001-186173, A (Matsushita Electric Industrial Co., Ltd.), July 6, 2001 (07.06.01), Paragraph No. [0153]

Document 13: JP, 2002-232955, A (Denso Corporation), August 16, 2002 (08.16.02), Claims 1-3

Document 14: JP, 2001-86110, A (Toyo Communication Equipment Co., Ltd.), March 30, 2001 (03.30.01), Paragraph No. [0005], Fig. 9

## Claims 52-54, 65-67, 75-77 and 80-82

Each of the above documents 1 and 2 describes key exchange between a transmission device and reception device, and based on the key exchanged by the key exchange, encrypting the data, and transmitting and receiving the same.

Also, using transmission-related information such as a sending address and transmission/reception managing information such as a MAC address to generate a packet is generally carried out in an IP network.

Also, documents 3 and 4 describe that, when buffer storage capacity exceeds threshold, data in the buffer is preferentially output.

When storage capacity exceeds a threshold, controlling by preferentially outputting data so that storage capacity declines below the threshold is the same as controlling so that storage capacity does not exceed the threshold.

Document 5 describes accumulating packets in a plurality of class queues, and in accordance with bandwidth information allocated to the class, outputting the packets accumulated in each queue.

## Claims 55-64

Document 6 describes transmitting important data encrypted and data of low important without encryption.

Controlling the data transmission rate of data so as not to decline below a prescribed value is generally carried out in shaping and the like.

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.  
Continuation of Box V.2:

## Claim 60

Document 7 describes outputting data so as not to exceed remaining accumulation time, that is, outputting data so that the accumulation time is shorter than a value set in advance.

## Claims 61-64 and 79

Document 8 describes checking the maximum transmissible packet length in a transmission route from transmission device to reception device, and transmitting data at maximum packet length.

Attaching to a packet data on packet length for transmission and data for error correction is generally carried out.

## Claim 69, 73, 90 and 93

Document 9 describes that when a key has been used for a prescribed time, the key is updated.

Under what protocols a key is to be updated every set time frame is a matter of design that could be determined as appropriate by a party skilled in the art, and no particular difficulty is found in adopting a known RTP as a protocol.

## Claims 72 and 92

Document 10 describes updating a key for every time a set volume of data is processed.

Under what protocols a key is to be updated for every time a set volume of data is processed is a matter of design that could be determined as appropriate by a party skilled in the art, and no particular difficulty is found in adopting a known HTTP as a protocol.

## Claim 78

Document 11 describes outputting packets evenly from a plurality of queues.

## Claims 83 and 84

Document 12 describes using a TOS field for an Ipv4 packet and a traffic class field for an Ipv6 packet as fields for packet priority.

## Claims 85-89

Document 13 describes performing authentication in accordance with position information of a mobile terminal, and if authentication is denied, performing authentication using a password.

A constitution such that authentication is made using a certificate or and the like in place of authentication using a password could be easily conceived of by a party skilled in the art.

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.  
Continuation of Box V.2:

## Claim 91

Document 14 describes adding key change timing to a transmission packet.

## Claim 68

None of the above documents 1-14 describes or suggests transmitting information indicating encryption key prior to the time from transmission of a transmission frame to reception of a reception frame corresponding thereto.

## Claims 70, 71, 74, 96 and 97

None of the above documents 1-14 describes or suggests setting key update timing to be timing synchronized to a sequence number, updating each HTTP request, setting a timing synchronized to an end or beginning of an error correction matrix, and notifying timing by a port number change.

## Claims 94 and 95

None of the above documents 1-14 describes or suggests performing authentication in accordance with one way or round-trip propagation delay time of a packet, and whether the mode is scrambled transmission.

## Claim 98

None of the above documents 1-14 describes or suggests transmitting DTCP system copy control information by adding encryption mode information to a transmission packet.